

06.03.00 #3

日 本 国 特 許 庁

PATENT OFFICE
JAPANESE GOVERNMENT

JP00/01333

REC'D 14 APR 2000

WIPO PCT

別紙添付の書類は下記の出願書類の謄本に相違ないことを証明する。
This is to certify that the annexed is a true copy of the following application as filed
with this Office.

出 願 年 月 日
Date of Application: 1999年3月19日

出 願 番 号
Application Number: PCT/JP99/1402号

出 願 人
Applicant(s): 株式会社日立製作所
北原 潤
朝日 猛

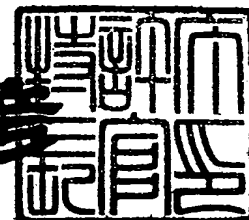
4

**PRIORITY
DOCUMENT**
SUBMITTED OR TRANSMITTED IN
COMPLIANCE WITH RULE 17.1(a) OR (b)

2000年 3 月 31 日

特許庁長官
Commissioner,
Patent Office


近 藤 隆 彦



特許協力条約に基づく国際出願

願 書

出願人は、この国際出願が特許協力条約に従って処理されることを請求する。

国際出願番号	受理官庁記入欄
国際出願日	
(受付印)	
出願人又は代理人の書類記号 (希望する場合は最大12字) 349900423971	

第I欄 発明の名称

情報処理装置

第II欄 出願人

氏名(名称)及びあて名:(姓・名の順に記載;法人は公式の完全な名称を記載;あて名は郵便番号及び国名も記載)

株式会社 日立製作所
HITACHI, LTD.
〒101-8010 日本国東京都千代田区神田駿河台四丁目6番地
6, Kanda Surugadai 4-chome, Chiyoda-ku,
TOKYO 101-8010 JAPAN

☐ この欄に記載した者は、
発明者でもある。

電話番号:

ファクシミリ番号:

加入電話番号:

国籍(国名): 日本国 JAPAN

住所(国名): 日本国 JAPAN

この欄に記載した者は、次の
指定国についての出願人である: ☐ すべての指定国 ☒ 米国を除くすべての指定国 ☐ 米国のみ ☐ 追記欄に記載した指定国

第III欄 その他の出願人又は発明者

氏名(名称)及びあて名:(姓・名の順に記載;法人は公式の完全な名称を記載;あて名は郵便番号及び国名も記載)

北 原 潤
KITAHARA Jun
〒215-0013 日本国神奈川県川崎市麻生区王禅寺1099番地
株式会社日立製作所 システム開発研究所内
C/O Systems Development Laboratory, HITACHI, LTD.
1099, Ouzenji, Asao-ku, Kawasaki-shi, KANAGAWA
215-0013 JAPAN

この欄に記載した者は、
次に該当する:

☐ 出願人のみである。

☒ 出願人及び発明者である。

☐ 発明者のみである。
(ここにレ印を付したとき
は、以下に記入しないこと)

国籍(国名): 日本国 JAPAN

住所(国名): 日本国 JAPAN

この欄に記載した者は、次の
指定国についての出願人である: ☐ すべての指定国 ☐ 米国を除くすべての指定国 ☒ 米国のみ ☐ 追記欄に記載した指定国

☒ その他の出願人又は発明者が続業に記載されている。

第IV欄 代理人又は共通の代表者、通知のあて名

次に記載された者は、国際機関において出願人のために行動する:

☒ 代理人 ☐ 共通の代表者

氏名(名称)及びあて名:(姓・名の順に記載;法人は公式の完全な名称を記載;あて名は郵便番号及び国名も記載)

6850 弁理士 小 川 勝 男
OGAWA Katsuo, Patent Attorney (Reg. NO. 6850)
〒100-8220 日本国東京都千代田区丸の内一丁目5番1号
株式会社日立製作所内
C/O HITACHI, LTD., 5-1, Marunouchi 1-chome, Chiyoda-ku,
TOKYO 100-8220 JAPAN

電話番号:

03-3212-1111

ファクシミリ番号:

03-3214-3116

加入電話番号:

☐ 通知のための宛名: 代理人又は共通の代表者が選任されておらず、上記枠内に特に通知が送付されるあて名を記載している場合は、レ印を付す

第Ⅲ欄の続き その他の出願人又は発明者

この続葉を使用しないときは、この用紙を願書に含めないこと。

氏名（名称）及びあて名：（姓・名の順に記載；法人は公式の完全な名称を記載；あて名は郵便番号及び国名も記載）

朝 日 猛

ASAHI Takeshi

〒215-0013 日本国神奈川県川崎市麻生区王禅寺1099番地

株式会社日立製作所 システム開発研究所内

C/O Systems Development Laboratory, HITACHI, LTD.

1099, Ouzenji, Asao-ku, Kawasaki-shi, KANAGAWA

215-0013 JAPAN

この欄に記載した者は、次に該当する：

☐ 出願人のみである。☒ 出願人及び発明者である。☐ 発明者のみである。
（ここにレ印を付したときは、以下に記入しないこと）

国籍（国名）： 日本国 JAPAN

住所（国名）： 日本国 JAPAN

この欄に記載した者は、次の指定国についての出願人である：

☐ すべての指定国☐ 米国を除くすべての指定国☒ 米国のみ☐ 追記欄に記載した指定国

氏名（名称）及びあて名：（姓・名の順に記載；法人は公式の完全な名称を記載；あて名は郵便番号及び国名も記載）

この欄に記載した者は、次に該当する：

☐ 出願人のみである。☐ 出願人及び発明者である。☐ 発明者のみである。
（ここにレ印を付したときは、以下に記入しないこと）

国籍（国名）：

住所（国名）：

この欄に記載した者は、次の指定国についての出願人である：

☐ すべての指定国☐ 米国を除くすべての指定国☐ 米国のみ☐ 追記欄に記載した指定国

氏名（名称）及びあて名：（姓・名の順に記載；法人は公式の完全な名称を記載；あて名は郵便番号及び国名も記載）

この欄に記載した者は、次に該当する：

☐ 出願人のみである。☐ 出願人及び発明者である。☐ 発明者のみである。
（ここにレ印を付したときは、以下に記入しないこと）

国籍（国名）：

住所（国名）：

この欄に記載した者は、次の指定国についての出願人である：

☐ すべての指定国☐ 米国を除くすべての指定国☐ 米国のみ☐ 追記欄に記載した指定国

氏名（名称）及びあて名：（姓・名の順に記載；法人は公式の完全な名称を記載；あて名は郵便番号及び国名も記載）

この欄に記載した者は、次に該当する：

☐ 出願人のみである。☐ 出願人及び発明者である。☐ 発明者のみである。
（ここにレ印を付したときは、以下に記入しないこと）

国籍（国名）：

住所（国名）：

この欄に記載した者は、次の指定国についての出願人である：

☐ すべての指定国☐ 米国を除くすべての指定国☐ 米国のみ☐ 追記欄に記載した指定国☐ その他の出願人又は発明者が続葉に記載されている。

欄 国の指定

規則 4.9(a)の規定に基づき次の指定を行う（該当する□内にレ印を付すこと；少なくとも1つの□にレ印を付すこと）。

広域特許

- ☐ **AP** **ARIPO**特許：GHガーナ Ghana, KEケニア Kenya, LSレソト Lesotho, MWマラウイ Malawi, SDスーダン Sudan, SZスワジランド Swaziland, UGウガンダ Uganda, ZWジンバブエ Zimbabwe, 及びハラレプロトコルと特許協力条約の締約国である他の国

☐ **EA** ユーラシア特許：AMアルメニア Armenia, AZアゼルバイジャン Azerbaijan, BYベラルーシ Belarus, KGキルギスタン Kyrgyzstan, KZカザフスタン Kazakhstan, MDモルドヴァ Republic of Moldova, RUロシア連邦 Russian Federation, TJタジキスタン Tajikistan, TMトルクメニスタン Turkmenistan, 及びユーラシア特許条約と特許協力条約の締約国である他の国

☒ **EP** ヨーロッパ特許：ATオーストリア Austria, BEベルギー Belgium, CH and LIスイス及びリヒテンシュタイン Switzerland and Liechtenstein, CYキプロス Cyprus, DEドイツ Germany, DKデンマーク Denmark, ESスペイン Spain, FIフィンランド Finland, FRフランス France, GB英国 United Kingdom, GRギリシャ Greece, IEアイルランド Ireland, ITイタリア Italy, LUルクセンブルグ Luxembourg, MCモナコ Monaco, NLオランダ Netherlands, PTポルトガル Portugal, SEスウェーデン Sweden, 及びヨーロッパ特許条約と特許協力条約の締約国である他の国

☐ **OA** **OAPI**特許：BFブルキナ・ファソ Burkina Faso, BJベニン Benin, CF中央アフリカ Central African Republic, CGコンゴ Congo, CI象牙海岸 Cote d'Ivoire, CMカメルーン Cameroon, GAガボン Gabon, GNギニア Guinea, MLマリ Mali, MRモーリタニア Mauritania, NEニジェール Niger, SNセネガル Senegal, TDチャード Chad, TGトーゴ Togo, 及びアフリカ知的所有権機構と特許協力条約の締約国である他の国（他の種類の保護又は取扱いを求める場合には点線の上に記載する）

国内特許 (他の種類の保護又は取扱いを求める場合には点線上に記載する)

- | | | | |
|--|---|--|--------------------------------|
| <input type="checkbox"/> AL | アルバニア Albania | <input type="checkbox"/> MN | モンゴル Mongolia |
| <input type="checkbox"/> AM | アルメニア Armenia | <input type="checkbox"/> MW | マラウイ Malawi |
| <input type="checkbox"/> AT | オーストリア Austria | <input type="checkbox"/> MX | メキシコ Mexico |
| <input type="checkbox"/> AU | オーストラリア Australia | <input type="checkbox"/> NO | ノールウェー Norway |
| <input type="checkbox"/> AZ | アゼルバイジャン Azerbaijan | <input type="checkbox"/> NZ | ニュー・ジーランド New Zealand |
| <input type="checkbox"/> BA | ボスニア・ヘルツェゴビナ Bosnia and Herzegovina | <input type="checkbox"/> PL | ポーランド Poland |
| | | <input type="checkbox"/> PT | ポルトガル Portugal |
| <input type="checkbox"/> BB | バルバドス Barbados | <input type="checkbox"/> RO | ルーマニア Romania |
| <input type="checkbox"/> BG | ブルガリア Bulgaria | <input type="checkbox"/> RU | ロシア連邦 Russian Federation |
| <input type="checkbox"/> BR | ブラジル Brazil | <input type="checkbox"/> SD | スーダン Sudan |
| <input type="checkbox"/> BY | ベラルーシ Belarus | <input type="checkbox"/> SE | スウェーデン Sweden |
| <input type="checkbox"/> CA | カナダ Canada | <input checked="" type="checkbox"/> SG | シンガポール Singapore |
| <input type="checkbox"/> CH | and LI スイス及びリヒテンシュタイン
Switzerland and Liechtenstein | <input type="checkbox"/> SI | スロヴェニア Slovenia |
| <input checked="" type="checkbox"/> CN | 中国 China | <input type="checkbox"/> SK | スロヴァキア Slovakia |
| <input type="checkbox"/> CU | キューバ Cuba | <input type="checkbox"/> SL | シエラレオネ Sierra Leone |
| <input type="checkbox"/> CZ | チェッコ Czech Republic | <input type="checkbox"/> TJ | タジキスタン Tajikistan |
| <input type="checkbox"/> DE | ドイツ Germany | <input type="checkbox"/> TM | トルクメニスタン Turkmenistan |
| <input type="checkbox"/> DK | デンマーク Denmark | <input type="checkbox"/> TR | トルコ Turkey |
| <input type="checkbox"/> EE | エストニア Estonia | <input type="checkbox"/> TT | トリニダード・トバゴ Trinidad and Tobago |
| <input type="checkbox"/> ES | スペイン Spain | <input type="checkbox"/> UA | ウクライナ Ukraine |
| <input type="checkbox"/> FI | フィンランド Finland | <input type="checkbox"/> UG | ウガンダ Uganda |
| <input type="checkbox"/> GB | 英国 United Kingdom | <input checked="" type="checkbox"/> US | 米国 United States of America |
| <input type="checkbox"/> GE | グルジア Georgia | <input type="checkbox"/> UZ | ウズベキスタン Uzbekistan |
| <input type="checkbox"/> GH | ガーナ Ghana | <input type="checkbox"/> VN | ヴィエトナム Viet Nam |
| <input type="checkbox"/> HU | ハンガリー Hungary | <input type="checkbox"/> YU | ユーゴスラビア Yugoslavia |
| <input type="checkbox"/> IL | イスラエル Israel | <input type="checkbox"/> ZW | ジンバブエ Zimbabwe |
| <input type="checkbox"/> IS | アイスランド Iceland | | |
| <input checked="" type="checkbox"/> JP | 日本 Japan | | |
| <input type="checkbox"/> KE | ケニア Kenya | | |
| <input type="checkbox"/> KG | キルギスタン Kyrgyzstan | | |
| <input checked="" type="checkbox"/> KR | 韓国 Republic of Korea | | |
| <input type="checkbox"/> KZ | カザフスタン Kazakhstan | | |
| <input type="checkbox"/> LC | セントルシア Saint Lucia | | |
| <input type="checkbox"/> LK | スリ・ランカ Sri Lanka | | |
| <input type="checkbox"/> LR | リベリア Liberia | | |
| <input type="checkbox"/> LS | レソト Lesotho | | |
| <input type="checkbox"/> LT | リトアニア Lithuania | | |
| <input type="checkbox"/> LU | ルクセンブルグ Luxembourg | | |
| <input type="checkbox"/> LV | ラトヴィア Latvia | | |
| <input type="checkbox"/> MD | モルドヴァ Republic of Moldova | | |
| <input type="checkbox"/> MG | マダガスカル Madagascar | | |
| <input type="checkbox"/> MK | マケドニア旧ユーゴスラヴィア The former Yugoslav Republic
of Macedonia | | |

以下の□は、この様式の施行後に特許協力条約の締約国となった国を指定
(国内特許のために) するためのものである

以下の□は、この様式の施行後に特許協力条約の締約国となった国を指定
(国内特許のために) するためのものである

出願人は、上記の指定に加えて、規則 4. 9 (b) の規定に基づき、特許協力条約の下で認められる全ての国の指定を行う。

ただし、この国の指定を除く。
 申請人は、これらの追加される指定が確認を条件としていること、並びに優先日から15月が経過する前にその確認がなされない指定は、この期間の経過時に、申請人によって取り下げられたものとみなされることを宣言する。（指定の確認は、指定を特定する通知の提出と指定手数料及び確認手数料の納付からなる。この確認は、優先日から15月以内に受理官庁へ提出されなければならない。）

欄 優先権主張

☐ 他の優先権の主張（先の出願）が追記欄に記載されている

この先の出願に基づき優先権を主張する		先の出願		
先の出願の出願日 (日、月、年)	先の出願の出願番号	国内出願：国名	広域出願：*広域官庁名	国際出願：受理官庁名
(1)				
(2)				
(3)				

☐ 上記（ ）の番号の先の出願（ただし、本国際出願が提出される受理官庁に対して提出されたものに限り）のうち、次の（ ）の番号のものについては、出願書類の認証謄本を作成し国際事務局へ送付することを、受理官庁（日本国特許庁の長官）に対して請求している。

*先の出願が、ARIPOの特許出願である場合には、その先の出願を行った工業所有権の保護のためのパリ条約同盟国の少なくとも1ヶ国を追記欄に表示しなければならない（規則4.10(b)(i)）。追記欄を参照。

第VII欄 国際調査機関

国際調査機関（ISA）の選択

ISA/J P

先の調査結果の利用請求；当該調査の照会

(先の調査が、国際調査機関によって既に実施又は請求されている場合)

出願日（日、月、年）

出願番号

国名（又は広域官庁）

第VIII欄 照合欄

この国際出願の用紙の枚数は次のとおりである。

願書	4	枚
明細書（配列表を除く）	15	枚
請求の範囲	3	枚
要約書	1	枚
図面	16	枚
明細書の配列表		枚
合計	39	枚

この国際出願には、以下にチェックした書類が添付されている。

- | | |
|---|---|
| 1. <input checked="" type="checkbox"/> 手数料計算用紙 | 5. <input type="checkbox"/> 優先権書類（上記第VI欄の（ ）の番号を記載する） |
| <input checked="" type="checkbox"/> 納付する手数料に相当する特許印紙を貼付した書面 | 6. <input type="checkbox"/> 国際出願の翻訳文（翻訳に使用した言語名を記載する） |
| <input type="checkbox"/> 国際事務局の口座への振込みを証明する書面 | 7. <input type="checkbox"/> 寄託した微生物又は他の生物材料に関する書面 |
| 2. <input checked="" type="checkbox"/> 別個の記名押印された委任状 | 8. <input type="checkbox"/> ヌクレオチド又はアミノ酸配列表（フレキシブルディスク） |
| 3. <input type="checkbox"/> 包括委任状の写し | 9. <input type="checkbox"/> その他（書類名を詳細に記載する） |
| 4. <input type="checkbox"/> 記名押印（署名）の説明書 | 優先権書類送付請求書 |

要約書とともに提示する図面 第 1 図

本国際出願の使用言語名： 日本語

第IX欄 提出者の記名押印

各人の氏名（名称）を記載し、その次に押印する。

小川 勝男



1. 国際出願として提出された書類の実際の受理の日	受理官庁記入欄	2. 図面
3. 国際出願として提出された書類を補充する書類又は図面であって その後期間内に提出されたものの実際の受理の日（訂正日）		<input type="checkbox"/> 受理された
4. 特許協力条約第11条(2)に基づく必要な補充の期間内の受理の日		<input type="checkbox"/> 不足図面がある
5. 出願人より特定された 国際調査機関	ISA/J P	6. <input type="checkbox"/> 調査手数料未払いにつき、国際調査機関 に調査用写しを送付していない

国際事務局記入欄

記録原本の受理の日

P C T

手数料計算用紙

願書附属書

受理官庁記入欄

国際出願番号

受理完了の日付印

出願人又は代理人の書類記号

3 4 9 9 0 0 4 2 3 9 7 1

出願人

株式会社 日立製作所

所定の手数料の計算

1. 及び2. 特許協力条約に基づく国際出願等に関する法律（国内法）
第18条第1項第1号の規定による手数料（注1）
（送付手数料【T】及び調査手数料【S】の合計）

95,000 円 T + S

3. 国際手数料（注2）

基本手数料

国際出願に含まれる用紙の枚数 39 枚

最初の30枚まで.....

54,800 円 b 1

9 × 1,300 円 =

11,700 円 b 2

30枚を越える用紙の枚数 用紙1枚の手数料

b 1 及び b 2 に記入した金額を加算し、合計額をBに記入

66,500 円 B

指定手数料

国際出願に含まれる指定数（注3） 6

6 × 12,600 円 =

75,600 円 D

支払うべき
指定手数料の数
（上限は11）（注4）

1 指定当たりの手数料（円）

B 及び D に記入した金額を加算し合計額をIに記入.....

142,100 円 I

4. 納付すべき手数料の合計

T + S 及び I に記入した金額を加算し、合計額を合計に記入

237,100 円

合 計

（注1）送付手数料及び調査手数料については、合計金額を特許印紙をもって納付しなければならない。

（注2）国際手数料については、受理官庁である日本国特許庁の長官が告示する国際事務局の口座への振込みを証明する書面を提出することにより納付しなければならない。

（注3）願書第V欄でレ印を付した口の数。

（注4）指定数を記入する。ただし、11指定以上は一律11とする。

明 細 書

情報処理装置

5

技術分野

本発明は、情報の保管、転送時の秘密性を保つために暗号を使用する情報処理装置に関する。その中でも特に、秘密性保持の高い情報処理を構築することに関する。

10

背景技術

暗号を使用する情報処理装置の従来技術としては、以下のものがある。

15

ハードディスクドライブのような外部記憶装置に、情報を暗号化して記憶するものとして、特開平10-275115号公報がある。特開平10-275115号公報では、外部記憶装置12に一旦書き込まれた暗号化データY a, Y bを情報端末装置11へ転送する過程で、暗号化・復号鍵蓄積部35に蓄積された復号鍵K bを用いながら当該暗号化データY a, Y bに逐次的に復号処理を施すものである。

20

また、情報処理装置内に専用の暗号処理装置を設けたものとして、特開平10-214233号公報がある。特開平10-214233号公報では、携帯型P Cの中にデータを暗号化して暗号化ファイルのボディ部を生成する暗号化装置を備えている。

25

ここで、暗号化や復号化といった暗号処理は、一般に主記憶上のデータを対象に処理するため、主記憶上に秘密にすべきデータが存在する。情報を暗号化するためには、暗号アルゴリズムに従い情報を処理しなければならないが、暗号アルゴリズムと暗号に用いる鍵情報と暗号をかける秘密情

報全てを、安全に処理する必要が生じる。

しかし、これらの従来技術では以下の問題が存在する。

従来技術においては、秘密情報や暗号処理の途中経過が主記憶上に存在するため、幾つかの手法で情報を取り出す事が可能になる問題がある。この問題は、CPU や主記憶などが、複数の半導体で構成されている情報処理装置において、CPU を用いて暗号処理を行うと暗号アルゴリズムや暗号をかける秘密情報や暗号処理の途中経過が主記憶上に存在するためである。

また、情報処理装置内には、情報処理装置を構成する各半導体部品を接続する信号線（例えばバス）が存在するため、この信号線を観察し、情報を解析する事により、暗号化する前のデータや復号化したデータを簡単に取り出せるという問題がある。

発明の開示

上記の問題を解決するために、本発明では、以下の構成とした。

情報処理装置を構成する半導体内部で暗号化処理を施す。また、情報処理装置内の信号線上に暗号に関する情報を出力しない。情報処理装置の信号線上には、他者に観察されてもかまわない情報が出力される。この情報としては、暗号化された情報や暗号化する必要のない情報などである。なお、暗号に関する情報としては、暗号化されていない情報や暗号化された情報を復号するための情報を含む。

より具体的には、本発明の構成は、情報処理装置での処理を実行する処理装置（CPU）と同一半導体チップに、RAMと暗号処理アルゴリズムと暗号処理ハードウェアを集積したものである。なお、本明細書では便宜上CPUと読んでいるが、名称はこれに限られず、情報処理装置を構成する半導体チップであればよい。その中でも特に、情報処理装置の制御や演算処理を行う処理装置がよい。つまり、本発明は、情報処理装置を構成する1半導

体チップ内で暗号化処理が閉じているものである。さらに、本発明では、CPUが複数個あり、それぞれにおいて、暗号化処理が行う構成としてもよい。

また、この暗号処理が内蔵するRAM内で処理されてもよい。

5 また、CPUに内蔵されるRAMを主記憶として用い、アプリケーションプログラムの実行も内蔵するRAM内で処理されるものでもよい。

また、アプリケーションプログラム自体も暗号化され、外部記憶装置には、暗号化ファイルが存在する構成にしたものでもある。

10 また、外部バスへのデータ出力を制御する外部バス制御部を設けてもよい。この外部バス制御部では、内部RAMがアクセスされているときのデータを外部バスへ出力しないよう制御してもよい。さらに、このデータ外部バスに出力してもよい情報か否かを判断して、出力してもよい場合にデータを外部バスに出力するように制御してもよい。

また、通信データの暗号化／復号化をCPU内部で処理するものである。

15 さらに、これらのいずれかの構成に、情報に応じて暗号化するか否かを決定してもよい。情報が、暗号化しなくともよい情報であれば暗号化せずに情報処理装置の信号線上に出力する構成としてもよい。

さらに、本発明は、ディスクシステムコントローラ内のプロセッサ内部で暗号処理を可能にすることで、磁気ディスク上のファイル配置情報を暗号化したものも含まれる。

20

図面の簡単な説明

第1図は、本発明の情報処理装置の構成を示す図である。第2図は、本発明の情報処理装置におけるファイル生成を説明する図である。第3図は、本発明の1形態である主記憶を内蔵するCPUを有する情報処理装置の構成を示す図である。第4図は、本発明の1形態である外部記憶装置に格納して

25

いるアプリケーションプログラムをCPUで暗号化する情報処理装置の構成を

示す図である。第5図は、外部バス制御部の構成を示す図である。第6図は、外部バス制御部で外部バスへのデータを出力させない1実施例を説明する図である。第7図は、本発明をプロセッサバスおよびシステム情報処理装置に適用した場合の構成を示す図である。第8図は、本発明を通信に適用した場合の構成を示す図である。第9図は、外部記憶装置に本発明を適用した場合を説明する図である。第10図は、第9図の構成で暗号化ファイル配置情報の書込みを説明する図である。第11図は、ディスクコントローラの構成を示す図である。第12図は、本発明の1形態である複数のCPUを有する情報処理装置を示す図である。第13図は、第12図の変形例を示す図である。第14図は、第9図に示した構成の変形例である。第15図は、第9図に示した構成の変形例である。第16図は、第8図に示す情報処理装置がネットワークに接続されている全体システムを表わす図である。

15 発明を実施するための最良の形態

以下、図面を用いて本発明の実施例を説明する。

まず、本発明の第一の実施例を第1図および第2図を用いて説明する。第1図は、少なくとも、CPU(102)、主記憶装置(103)、外部記憶装置(104)を備える情報処理装置(101)の構成を模式的に表した図である。CPU(102)、主記憶装置制御部(117)、外部記憶装置制御部(115)は、理論上のシステムバス(114)で接続され、各々に主記憶装置(103)、外部記憶装置(104)が接続される。実際の信号線の接続は、第7図のようになるが、データの流れを理論的に考えると、模式的に第1図のように表す事が出来る。

CPU(102)は、マイクロプロセッサ(105)と、暗号処理アルゴリズムROM(106)と、暗号処理ハードウェア(107)と、RAM(108)と、鍵保管領域(112)と、外部バス制御部(109)からなる。さらに、同一半導体チップ上に

集積する。

CPU(102)内部では、マイクロプロセッサバス(110)に、暗号処理アルゴリズム ROM(106)と、暗号処理ハードウェア(107)と、RAM(108)と、外部バス制御部(109)が接続される。本実施例においては、CPU 内部でデータに対する暗号化処理が行われる。

ファイル(111)を暗号化するには、暗号処理アルゴリズム ROM(106)に従い、必要であれば暗号処理ハードウェア(107)を用いて暗号化する。この時の暗号化に用いる鍵データは、CPU(102)内で生成しても良いし、あらかじめ与えられるデータを用いても良い。但し、この鍵データは CPU(102)内の鍵保管領域(112)、保持されていなければならない。暗号化処理において、途中経過のデータが生成される場合は、その途中経過のデータも RAM(108)内に格納する。このようにして、ファイル(111)から暗号化ファイル(113)を生成する。

暗号化ファイル(113)は、システムバス(114)を通して外部記憶装置制御部(115)を経由して外部記憶装置(104)に格納する。

外部記憶装置(104)に格納されている暗号化ファイル(116)を復号化する場合は、逆の順序で処理を行う。

まず、外部記憶装置(104)から暗号化ファイル(116)を外部記憶装置制御部(115)を経由して RAM(108)に読み込む。次に、暗号処理アルゴリズム ROM(106)に従い、必要であれば暗号処理ハードウェア(107)を用いて復号化する。

大量のデータを高速に暗号化／復号化するためには、暗号鍵と復号鍵が共通である共通鍵暗号系を用いる。共通鍵暗号系では、暗号と復号は処理の順序が逆になっているだけで、最小単位の処理自体は暗号化も復号化も同じである。暗号処理アルゴリズム ROM(106)には、復号化処理の手順も格納しておく。また、暗号処理ハードウェア(107)は復号化でも使用する事が

可能である。

第2図は、第1図のファイル(111)を生成するまでの過程を示したものである。

アプリケーションプログラム(201)は、稼動時以外は外部記憶装置内に格納されている。このアプリケーションプログラムに起動がかかると主記憶に展開され動作可能な状態になる。動作可能になったアプリケーションプログラム(202)は、オペレーティングシステム等への情報処理装置管理プログラムに対して、作業領域の割り当てを要求する。このとき、オペレーティングシステム等への情報処理装置管理プログラムは、作業領域(203)としてRAM(108)内の空間を割り当てる。

この状態で、アプリケーションプログラム(202)は、マイクロプロセッサ(105)で処理され、生成された情報は作業領域(203)に格納される。この生成された情報の中から外部記憶装置に格納すべきデータをファイル(111)として生成する。

アプリケーションプログラム(202)自体は主記憶上に存在し、そのアプリケーションプログラムの作業領域(203)をRAM(108)上を取るためには、オペレーティングシステム等への情報処理装置管理プログラムが管理するマイクロプロセッサが持つメモリ管理機能を用い、アプリケーションプログラムの作業領域を示す論理アドレスをRAM(108)内の物理アドレスに変換する事で可能になる。

鍵保持部(112)は、RAM(108)の領域内に設けられていても良いが、不揮発性でなければならない。EEPROM や FlashROM のような不揮発性の ROM で構成しても良いし、バッテリバックアップされた SRAM で構成しても良い。バッテリバックアップされた SRAM で構成した場合、暗号に使用した鍵を取り出そうと、情報処理装置に攻撃が加えられた場合にそれを検知し、バックアップ電源を切断する事で、鍵情報を消失させ秘密情報を守ることにも可能

になる。

このように、情報の生成、暗号処理を同一半導体チップ内で行う事により、半導体チップの端子等の信号を観察するような解析方法でも、暗号のかからない秘密情報を入手する事は困難になる。

5 次に、本発明の第二の実施例を第3図を用いて説明する。

第3図は、CPU(101)内のRAM(108)を、情報処理装置(101)の主記憶として構成したものである。

10 この場合、外部記憶装置に格納されているアプリケーションプログラム(301)は、起動時にRAM(108)に展開され動作可能になる。動作可能になったアプリケーションプログラム(302)は、オペレーティングシステム等への情報処理装置管理プログラムに対して、作業領域の割り当てを要求する。このとき、オペレーティングシステム等への情報処理装置管理プログラムは、作業領域(303)としてRAM(108)内の空間を割り当てる。この状態で、アプリケーションプログラム(302)は、マイクロプロセッサ(105)で処理され、生成された情報は作業領域(303)に格納される。この生成された情報の中から外部記憶装置に格納すべきデータをファイル(111)として生成する。

15 生成されたファイル(111)は、暗号処理アルゴリズムROM(106)に従い、必要であれば暗号処理ハードウェア(107)を用いて暗号化される。暗号化されたファイル(113)は、外部記憶装置に暗号化ファイル(116)として格納される。

20 第3図では、CPU外部の主記憶装置を図示していないが、秘密情報を生成するアプリケーションプログラムとそれ以外のアプリケーションプログラムを区別し、秘密情報を生成するアプリケーションプログラムの実行は、RAM(108)で行い、それ以外のアプリケーションプログラムは、従来通りCPU外部の主記憶装置で処理する構成を取っても良い。

25 このように、RAM(108)を主記憶にする事により、CPU(102)外部にはアプ

リケーションプログラム(301)を RAM(108)に展開する時のデータ転送しか発生せず、アプリケーションプログラム自体の処理も安全に行える。

本発明の第三の実施例を第4図を用いて説明する。

5 本実施例では、暗号化されたアプリケーションプログラム(401)を外部記憶装置(104)に格納している。このアプリケーションプログラムは、情報処理装置の CPU 内で復号化される。このため、バス(114)上には、復号化されたアプリケーションプログラムは出力されず、復号化されたアプリケーションプログラムは CPU 内部で閉じている。このため、他者がこのアプリケーションプログラムを観察することを防止できる。

10 以下、第三の実施例の詳細を説明する。外部記憶装置内の暗号化アプリケーションプログラム(401)は、起動時にバス(114)を通して情報処理装置内の RAM(108)に転送される。転送された暗号化アプリケーションプログラム(402)は、RAM(108)に展開される。展開された暗号化アプリケーションプログラム(402)は、RAM(108)内で復号化され、アプリケーションプログラム(403)になる。この状態でアプリケーションプログラム(403)が動作し、RAM(108)内の作業領域(404)を用いながら情報を生成する。生成された情報は必要な部分が選択され、ファイル(111)としてまとめられる。ファイル(111)を暗号化し、暗号ファイル(113)を生成する。暗号ファイル(113)を暗号ファイル(116)として外部記憶装置(104)に格納する。

20 このように、アプリケーションプログラム自体も暗号化ファイルの一つとして外部記憶装置に格納する事により、さらに安全性を高める事も出来る。

25 なお、この暗号化アプリケーションプログラム(401)を生成するためには、アプリケーションプログラム自体をファイル(111)として、暗号化を行うものである。

次に、第5図および第6図を用いて、本発明の外部バス制御部の説明を

する。

第一から第三の各実施例に用いられる外部バス制御部(109)は、CPU 内部と外部とのデータの入出力を制御するものである。例えば、マイクロプロセッサ(105)が行う、暗号処理のために暗号処理アルゴリズム ROM(106)又は、暗号処理ハードウェア(107)又は、RAM(108)へのアクセスを CPU(102)外部に出ないように制御する。但し、マイクロプロセッサ(105)のアクセスが CPU 外部に出力されても構わないものであれば、外部に出力されるよう制御してもよい。この場合、CPU 外部に出力されても構わないデータとしては、暗号処理を行わず他の情報処理装置に転送するデータなどがある。

外部バス制御部(501)は、マイクロプロセッサ(502)の制御バス(503)、アドレスバス(504)、データバス(505)と、CPU の外部へ出る外部制御バス(506)、外部アドレスバス(507)、外部データバス(508)の間にあり、外部制御バス生成部(509)と、アドレス比較部(510)と、アドレス方向制御部(512)と、データ方向制御部(513)と、マスク信号生成部(511)と、信号マスク部(514)(519)から構成される。

制御バス(503)と外部制御バス(506)は、マイクロプロセッサからのバスサイクル開始信号、バス方向指示信号、バスサイクル終了信号、バス調停信号等が通される。これらの信号によりバスサイクルが制御される。

外部制御バス生成部(509)は、マイクロプロセッサからのバスサイクル開始信号、バス方向指示信号、バスサイクル終了信号、バス調停信号等を監視する。外部制御バス生成部(509)は、マイクロプロセッサがバスアクセス権を所有しているか否かを判断し、その情報をアドレス方向制御部(512)に伝える。また、同じ情報をアドレス比較器(510)にも伝える。アドレス比較器(510)は、CPU(102)内部の暗号処理アルゴリズム ROM(106)、暗号処理ハードウェア(107)、RAM(108)が割り当てられているアドレスを把握しており、アドレスバス(504)又は、外部アドレスバス(507)から入力されるアド

レスと比較する。

外部制御バス生成部(509)が制御バス(503)からマイクロプロセッサがバスアクセス権を所有していると判断すると、アドレス比較器(510)はマイクロプロセッサからのアドレスを監視し、RAM(108)のアドレスへのアクセスと検出すると、外部制御バス生成部(509)に伝えるえ、外部バス制御信号を駆動させない。また、マスク信号生成部(511)にも伝え、信号マスク部(514)(519)にマスク信号を出力し、外部アドレスバス(507)、外部データバス(508)を駆動しないように制御する。もしくは、強制的にアドレスの値やデータの値を固定してしまう。

外部制御バス生成部(509)が制御バス(503)からマイクロプロセッサがバスアクセス権を所有していないと判断すると、アドレス比較器(510)は外部アドレスバスを監視し、RAM(108)のアドレスへのアクセスと検出すると、外部制御バス生成部(509)に伝える。外部制御バス生成部(509)は、制御バス(503)へこのバスサイクルを伝達しない。もしくは、信号マスク部(514)(519)にマスク信号を出力し、アドレスバス(504)、データバス(505)を駆動しないように制御する。または、強制的にアドレスの値やデータの値を固定してしまう。

アドレスの値やデータの値を固定する方法として、第6図のように、信号マスク部(601)のゲート(602)と信号マスク部(603)のゲート(604)のように、ゲートの論理を変える事により実現できる。

このように、アドレス信号マスク回路で、RAM(108)領域以外の読み書きされても問題ない領域にアドレスを変換する事も可能である。

これにより、CPU(102)内部の処理をCPU(102)のバスであるシステムバス(114)を観察する事で推測する事が不可能になる。よって、CPU(102)内部で行う暗号処理の安全性が高まる。

次に、本発明の第四の実施例を第7図を用いて説明する。

第7図は、一般的な情報処理装置の構成を模式的に表した図である。

情報処理装置(701)は、複数の半導体部品から構成されている。CPU(702)はプロセッサバス(704)で、キャッシュメモリと主記憶制御部(705)に接続される。主記憶制御部(705)は、システムバス制御部を含み、メモリバス(713)とシステムバス(707)が接続される。メモリバス(713)には、主記憶装置(706)が接続され、システムバス(707)には、外部記憶装置(708)、表示系制御部(710)、通信系制御部(711)、その他 I/O 制御部(712)が接続される。表示系制御部(710)は、専用バスで主記憶装置制御部&システムバス制御部(705)に接続されていても良い。外部記憶装置制御部(708)には、外部記憶装置(709)が接続される。

主記憶装置(706)のアドレス領域と、システムバス(707)に接続される各部分のアドレス領域は異なっているため、アドレスでアクセスすべき領域を判断し、主記憶装置制御部&システムバス制御部(705)が切り替えている。

このような、情報処理装置(701)では、情報処理装置を一つのシステムと捉えると、このシステム内の主となるプロセッサは、CPU(702)である。この CPU 内部で暗号化処理を閉じさせる。例えば、CPU(702)を図1のように、マイクロプロセッサ(105)と、暗号処理アルゴリズム ROM(106)と、暗号処理ハードウェア(107)と、RAM(108)と、鍵保管領域(112)と、外部バス制御部(109)で構成し、さらに、同一半導体チップ上に集積する。また、本発明は、第12図および第13図に示すとおり、複数のCPUを有する情報処理装置であってもよい。

本発明の第五の実施例を第8図を用いて説明する。

第8図は、情報処理装置が他の情報処理装置と接続され、通信可能である構成を示す図である。ここでは、第1図の外部記憶装置の代わりに、通信系制御部を設けた構成をとる。なお、通信系制御部は、情報処理装置の外に接続されていてもよい。

情報処理装置(801)は、CPU(802)と、通信系制御部(803)とを備え、システムバス(814)で接続される。CPU(802)は、マイクロプロセッサ(805)、暗号処理アルゴリズム ROM(806)、暗号処理ハードウェア(807)、RAM(808)、外部バス制御部(809)、鍵保管領域(812)から構成され、マイクロプロセッサバス(810)で接続される。

第 8 図では、情報処理装置は、CPU と通信系制御で構成されているが、他に主記憶や外部記憶装置等が備わっていても良い。通信系制御部(803)を経由した通信回線(804)の先に、外部記憶装置と同じ機能を持つ装置が接続されていても良いし、情報処理装置が接続されていても良い。

但し、通信回線(804)の先に接続される装置が、記憶装置か情報処理装置かで、暗号の掛け方が異なる。

通信回線の先に接続される装置が、外部記憶装置の場合、データを暗号化し、それを記憶装置に格納し、暗号化されたデータを記憶装置から読み出して復号化するものである。このため、暗号化に用いた鍵は、暗号化を行った情報処理装置の CPU だけが保持していれば良い。

通信回線の先に接続される装置が、情報処理装置の場合、通信回線を挟んで情報処理装置 A と情報処理装置 B が存在する。この場合、情報処理装置 A で情報を暗号化し、情報処理装置 B で情報を復号化する状況が生ずる。大量のデータを高速に暗号化／復号化するためには、共通鍵暗号系が適する。しかし、暗号化と復号化で同じ鍵を用いるため、情報処理装置 A と B で、同じ鍵を所有していなければならない。この同じ鍵を、情報処理装置 A と B であらかじめ設定しておいても良いし、暗号化したデータを送る前に、情報処理装置 A と B で相互を行い、暗号化に用いた鍵を共有する方法を取っても良い。相互認証にも暗号処理が用いられるため、これらの処理は、CPU 内部で処理される。

この情報処理装置 A と B がネットワークを介して接続されている様子を

第16図に示す。

RAM(808)内で、暗号化したデータを通信単位に再編集し、通信プロトコルに従い、通信系制御部(803)に転送する事により、安全な通信が可能になる。RAM(808)内で暗号化したデータを通信系制御部(803)に転送し、通信系
5 制御部(803)において、暗号化したデータを通信単位に再編集し、通信プロトコルに従い、通信路(804)にデータを送出しても良い。

本発明の第六の実施例を第9図、第10図、第11図、第14図および第15図を用いて説明する。

第9図は、磁気ディスク(901)等の外部記憶装置群を、ディスクシステム
10 コントローラ(902)が制御する構成を取り、ディスクシステムコントローラ(902)は、上位の情報処理装置であるホストシステム(903)に接続されている。

磁気ディスク(901)内には、ファイルとして記憶されているデータと、そのファイルが磁気ディスク上の何処に格納されているかを示すファイル配置
15 情報がある。PC等の小型情報処理装置では、ファイルとファイル配置情報を管理するファイルシステムプログラムを、小型情報処理装置のCPUが処理する場合もあるが、高速動作や高信頼性を実現するディスクシステムコントローラでは、ディスクシステムコントローラ自体がファイルとファイル配置情報を管理する場合もある。

本実施例は後者に適用したものである。ホストシステム(903)では、ファイル(904)とファイル識別子(905)で管理する。ファイル(904)が暗号化されて
20 てるか否かは、ホストシステムに依存し、ディスクシステムコントローラでは関知しなくて良い。ディスクシステムコントローラ(902)では、磁気ディスク(901)上のファイル配置情報(906)を暗号化して管理する。

本実施例での、ホストシステムが暗号化した暗号化ファイル(907)を読み
25 出すまでの動作を説明する。

まず、ホストシステムは、必要とする暗号化ファイルに対応するファイル識別子(905)をディスクシステムコントローラ(902)に送り、暗号化ファイルの読み出し要求を行う。読み出し要求を受けたディスクシステムコントローラ(902)は、磁気ディスク(901)から、暗号化されたファイル配置情報(906)を読み出し、ディスクシステムコントローラ(902)内で復号化し、ファイル配置情報(908)を取り出す。このファイル配置情報(908)内からファイル識別子(905)を検索し、実際のファイルの配置情報を得る。選ばれたファイル配置情報を用いて、要求された暗号化ファイル(907)を磁気ディスク(901)から読み出し、ホストシステム(903)へ転送する。

磁気ディスクにファイルを書き込む場合を第10図で説明する。ファイル配置情報(908)を得るまでは、前記暗号化ファイルの読み出し動作と同じである。ファイル配置情報(908)から、磁気ディスク(901)の空き状態を確認し、磁気ディスク(901)空き領域に暗号化ファイル(904)を書き込む。書き込み終了後、ファイル配置情報(908)を更新し、暗号化した後、磁気ディスク(901)に暗号化ファイル配置情報(1001)として書き込む。

第11図で、ディスクシステムコントローラの構成を説明する。

本発明のディスクシステムコントローラ(1101)は、内部にディスクシステムのCPU(1102)と、磁気ディスクインタフェース(1113)と、ホストシステムインタフェース(1104)を持ち、CPU(1102)は、マイクロプロセッサ(1105)と、暗号処理アルゴリズムROM(1106)と、暗号処理ハードウェア(1107)と、RAM(1108)と、鍵保管領域(1111)と、外部バス制御部(1109)で構成される。

なお、第14図および第15図に示す通り、1台の情報処理装置に複数の磁気ディスク装置が接続される構成としてもよい。

このような、ディスクシステムコントローラを用いる事により、磁気ディスク内の情報を全て暗号化する事が可能になり、情報保管時の安全性

が高まる。

本発明の暗号処理ハードウェアは、暗号化と復号化において共通の鍵を用いる共通鍵暗号では、専用のハードウェアであり、ローテータ、加算器、論理演算器等で構成される。共通鍵暗号としては、あるデータ長を単位に、
5 ビットのローテートと加算と論理演算を主演算とした暗号化手段である Multi 系の暗号、M6 暗号等を用いる事も出来る。

公開鍵暗号を用いる場合は、演算量の大きい剰余演算器を専用のハードウェアとして設ける。

10 産業上の利用可能性

本発明によれば、情報処理装置内のシステムバスやプロセッサバスにも秘密情報を出さずに、暗号処理が可能になる。

暗号処理とその処理に関する秘密情報、暗号アルゴリズム、途中経過、鍵情報等が、同一半導体内で処理されるため、秘密保持効果が高い情報処理
15 装置を構築できる。

請 求 の 範 囲

1. 情報に対して所定の処理を施す制御装置と、

5 前記制御装置と当該情報処理装置を構成する他の装置を接続するバスを有する情報処理装置において、

前記制御装置は、暗号化すべき情報の暗号化を当該制御装置を含む半導体チップ内で実行することを特徴とする情報処理装置。

2. 請求項 1 に記載の情報処理装置において、

10 前記制御装置は、暗号化されていない情報を前記バスへの出力されないよう制御する外部バス制御装置を有することを特徴とする情報処理装置。

3. 請求項 2 に記載の情報処理装置において、

前記外部バス制御装置は、暗号化しなくともよい情報は、前記バスへ出力することを特徴とする情報処理装置。

15 4. 請求項 1 に記載の情報処理装置において、

前記制御装置で暗号化された情報を格納する記憶装置を有することを特徴とする情報処理装置。

5. 請求項 1 に記載の情報処理装置において、

20 前記制御装置は、暗号化された情報を復号化する手段を有することを特徴とする手段を有することを特徴とする情報処理装置。

6. 請求項 5 に記載の情報処理装置において、

ネットワークを介して他の情報処理装置と接続され、他の情報処理装置で暗号化されて送信された情報を前記制御装置で復号化することを特徴とする情報処理装置。

25 7. 請求項 1 に記載の情報処理装置において、

前記処理装置を複数個有し、夫々の処理装置にて暗号化を行うことを特

徴とする情報処理装置。

8. 請求項1に記載の情報処理装置において、

前記処理装置は、暗号化されたプログラムを受信し、復号化を施す手段を有することを特徴とする情報処理装置。

5 9. 請求項1に記載の情報処理装置において、

前記処理装置は、前記所定の処理を実行するマイクロプロセッサと、
前記情報の暗号化処理のアルゴリズムが格納された暗号処理アルゴリズム格納装置と、

前記アルゴリズムに従って暗号化処理を実行する暗号化装置と、

10 前記マイクロプロセッサ、暗号処理アルゴリズム格納装置および前記暗号化装置それぞれを接続するマイクロプロセッサバスと
を有することを特徴とする情報処理装置。

10. 情報を処理する処理装置を有し、暗号化された暗号化情報を格納する磁気ディスクを制御するディスクシステムコントローラにおいて、

15 前記暗号化情報の読み出し要求を受け取った場合、前記磁気ディスクに格納された情報の配置を示す暗号化されている暗号化ファイル配置情報を、
前記磁気ディスクから読み出し、読み出した暗号化ファイル配置情報を前記処理装置を含む半導体チップ内で復号化をし、復号化されたファイル配置情報に基づいて、前記暗号化情報を読み出すことを特徴とするディスク
20 システムコントローラ。

11. 請求項10に記載ディスクシステムコントローラにおいて、

1 当該複数の磁気ディスクに接続されていることを特徴とするディスクシステムコントローラ。

12. 請求項10に記載ディスクシステムコントローラにおいて、

25 当該ディスクシステムコントローラは、情報処理装置に接続されており、
前記情報処理装置からの要求により、前記暗号化情報を読み出すことを特

徴とするディスクシステムントローラ。

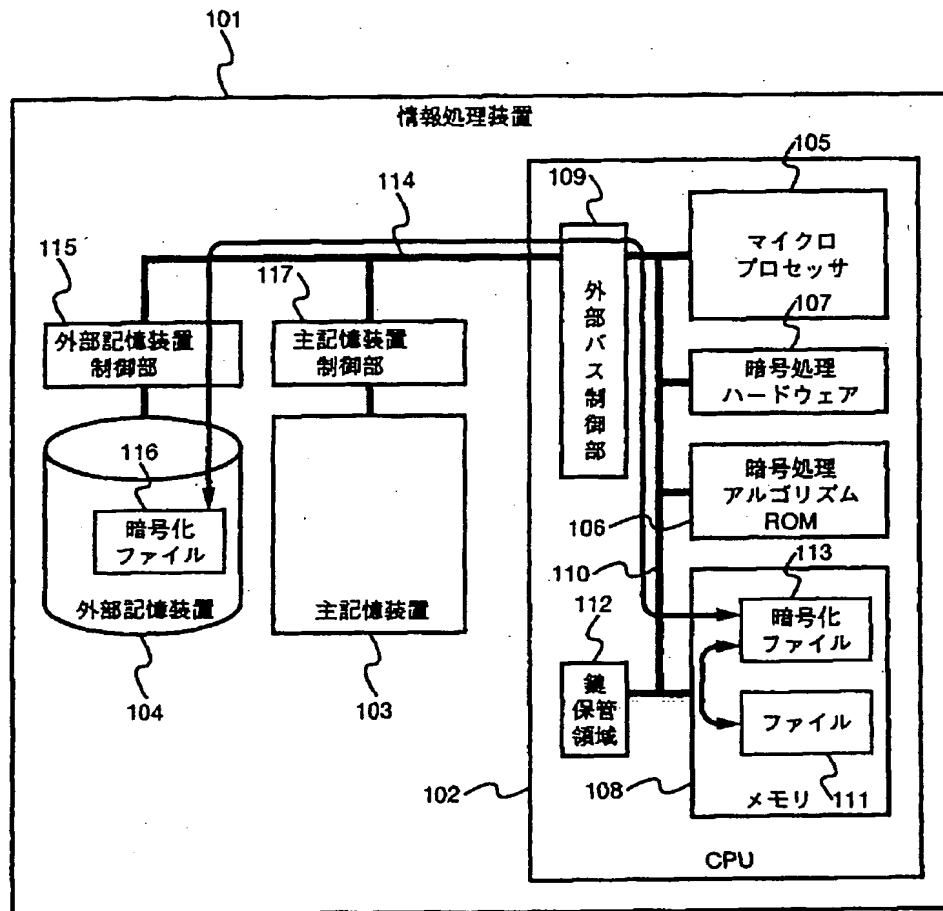
要 約 書

5 本発明は、秘密保持のために、情報を暗号化／復号化する情報処理装置や通信装置やファイル管理装置において、安全に暗号化／復号化を行う装置構成を提供するものである。

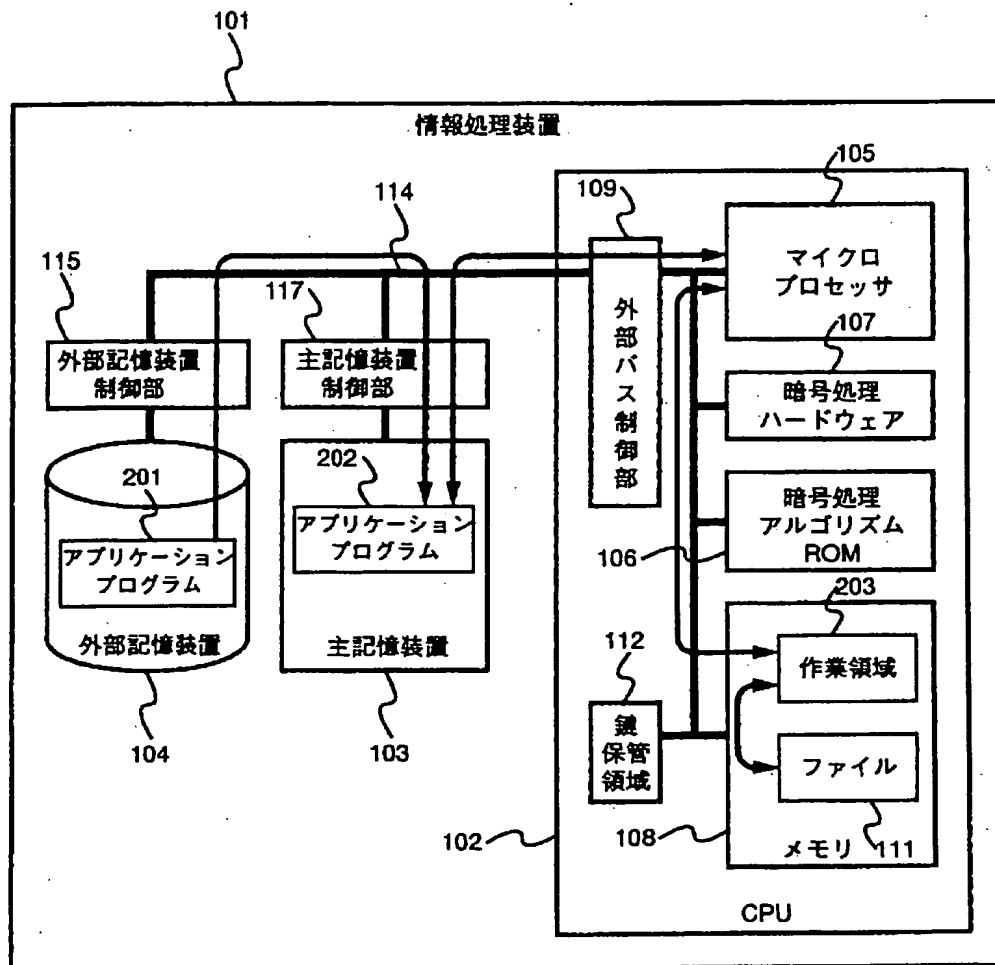
これらの装置は、複数の半導体部品から構成されている。そのため、装置内のシステムバスや主記憶を構成する半導体記憶素子に秘密にすべきデータが存在してしまう問題点がある。

10 そこで、本発明は以下の構成をとる。各装置のCPUに、マイクロプロセッサと、暗号処理アルゴリズムROMと、暗号処理ハードウェアと、RAMと、鍵保管領域と、外部バス制御部を設けさらに同一半導体チップ上に集積する。このCPUを内でのみ暗号化／復号化処理を行い、さらにCPU内部動作をCPU外部信号から推測不可能にする。

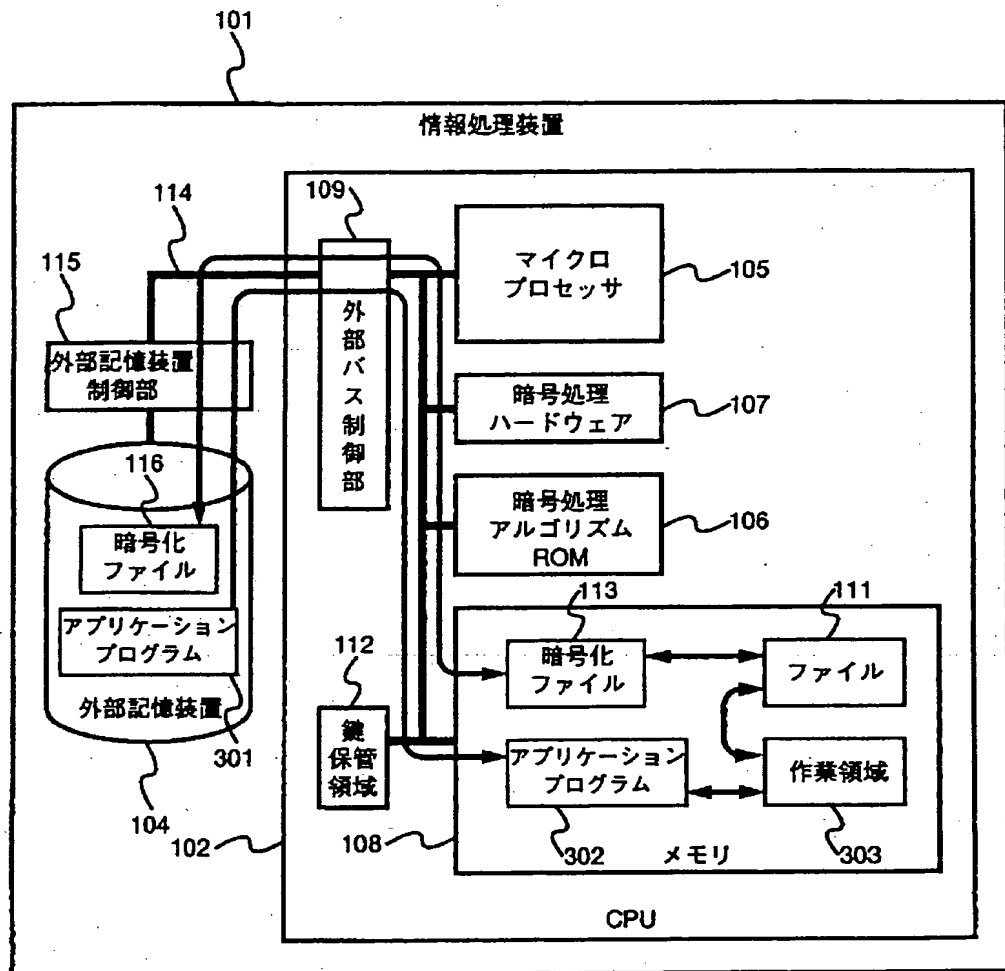
第1図



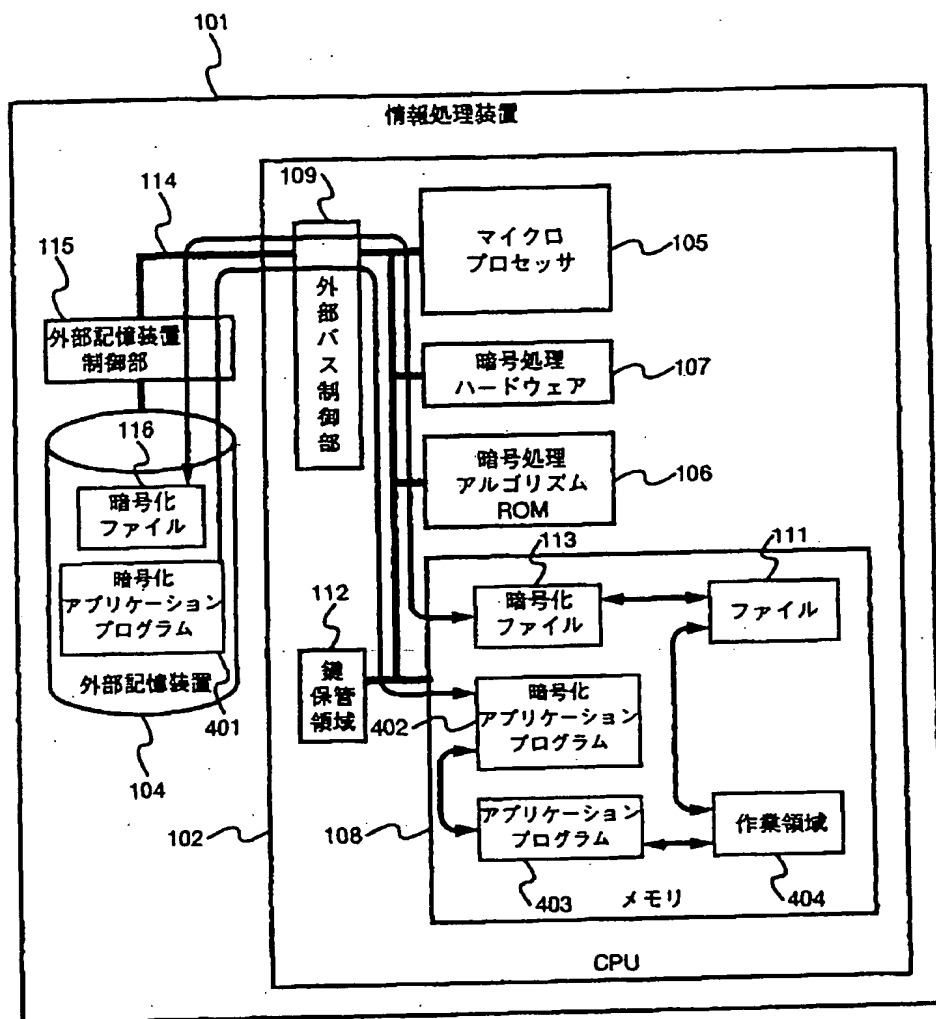
第2図



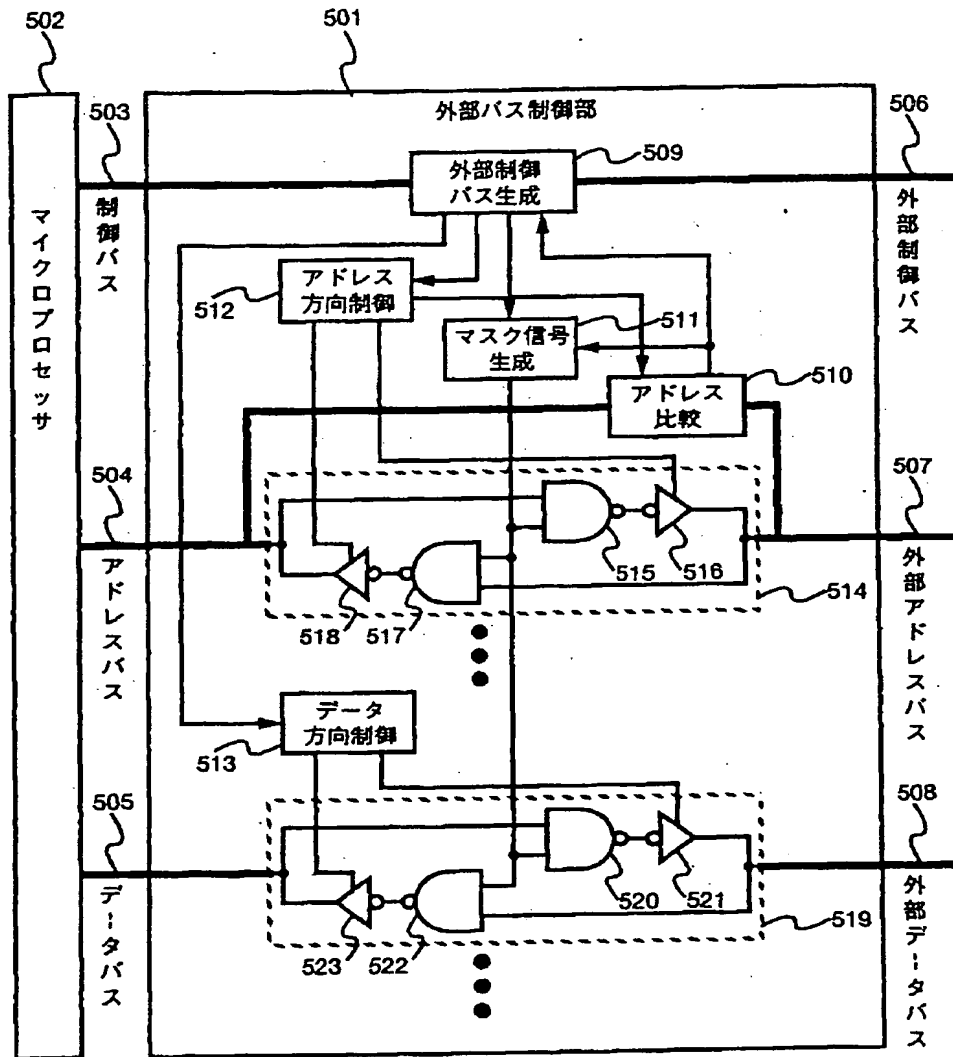
第3図



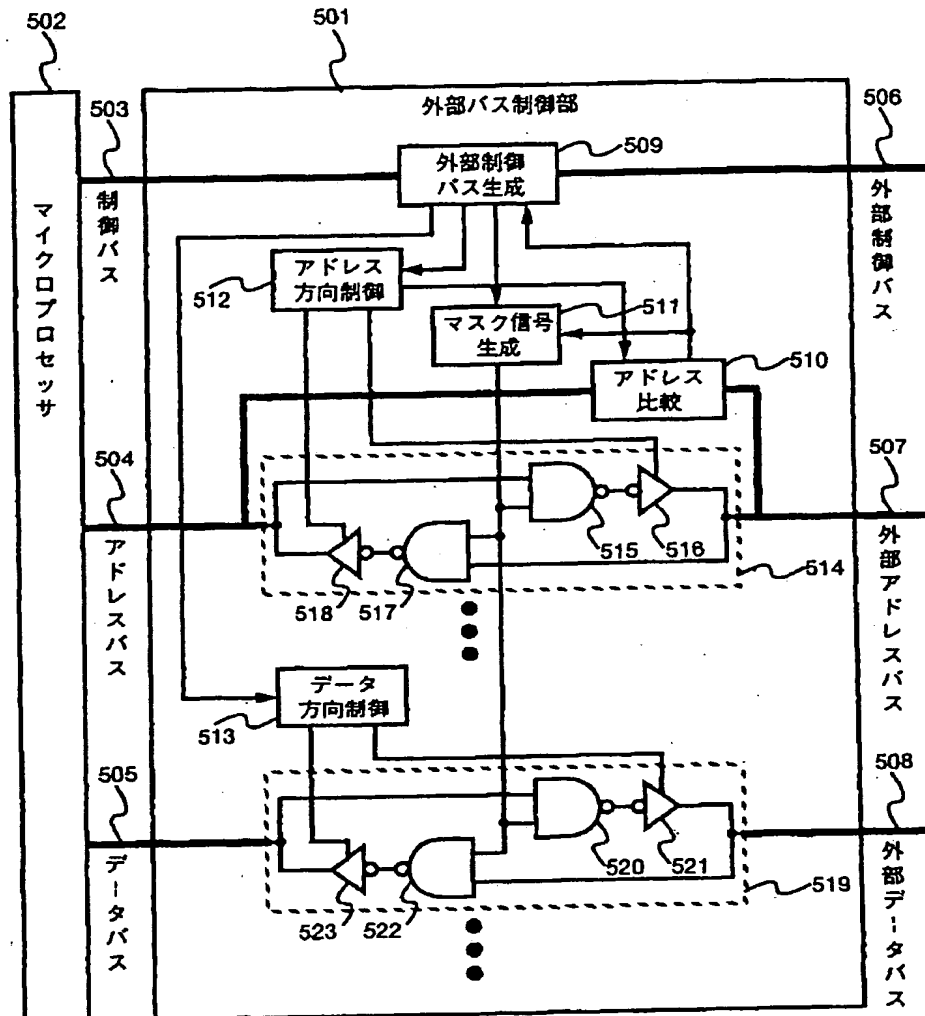
第4図



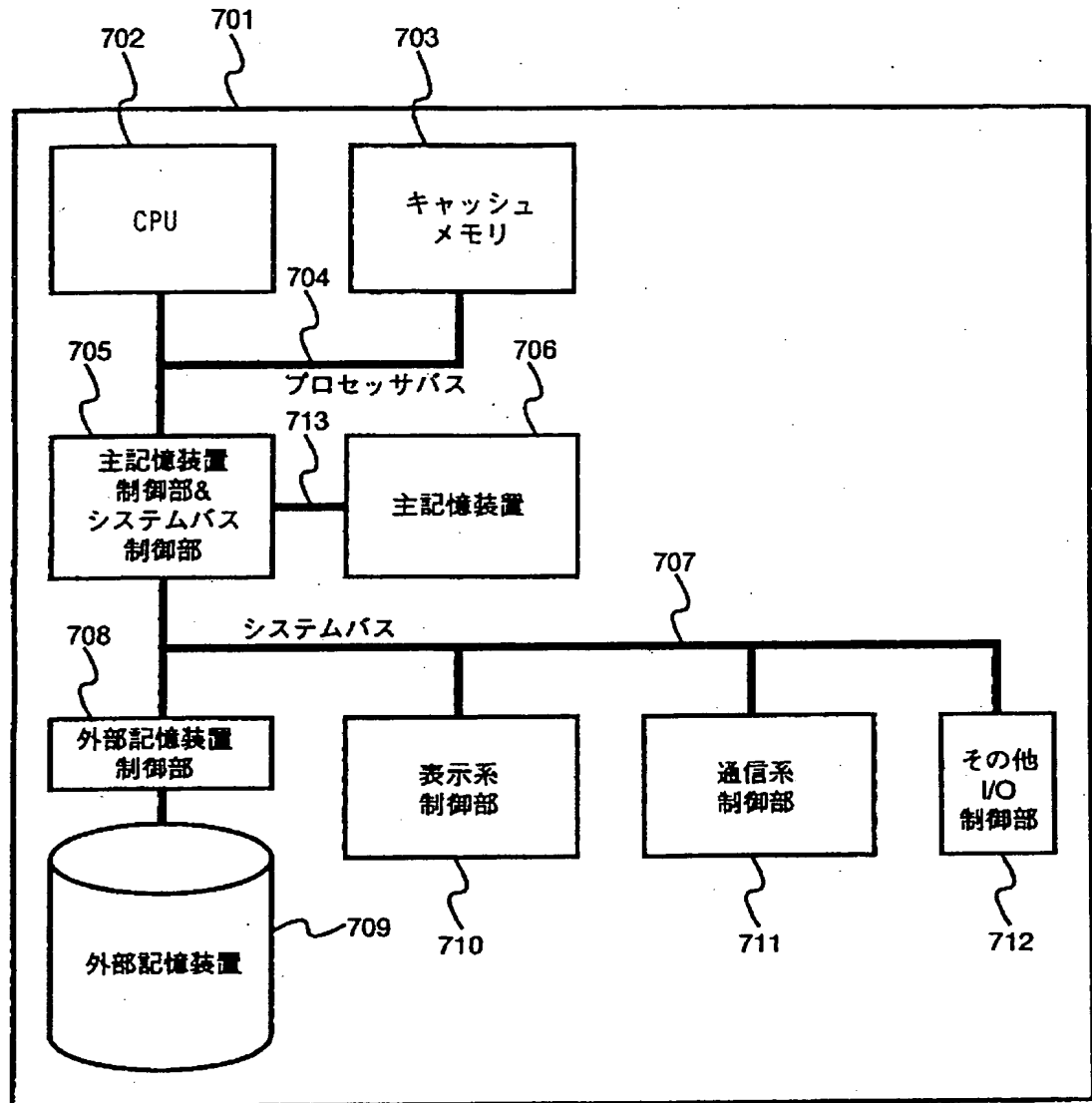
第5図



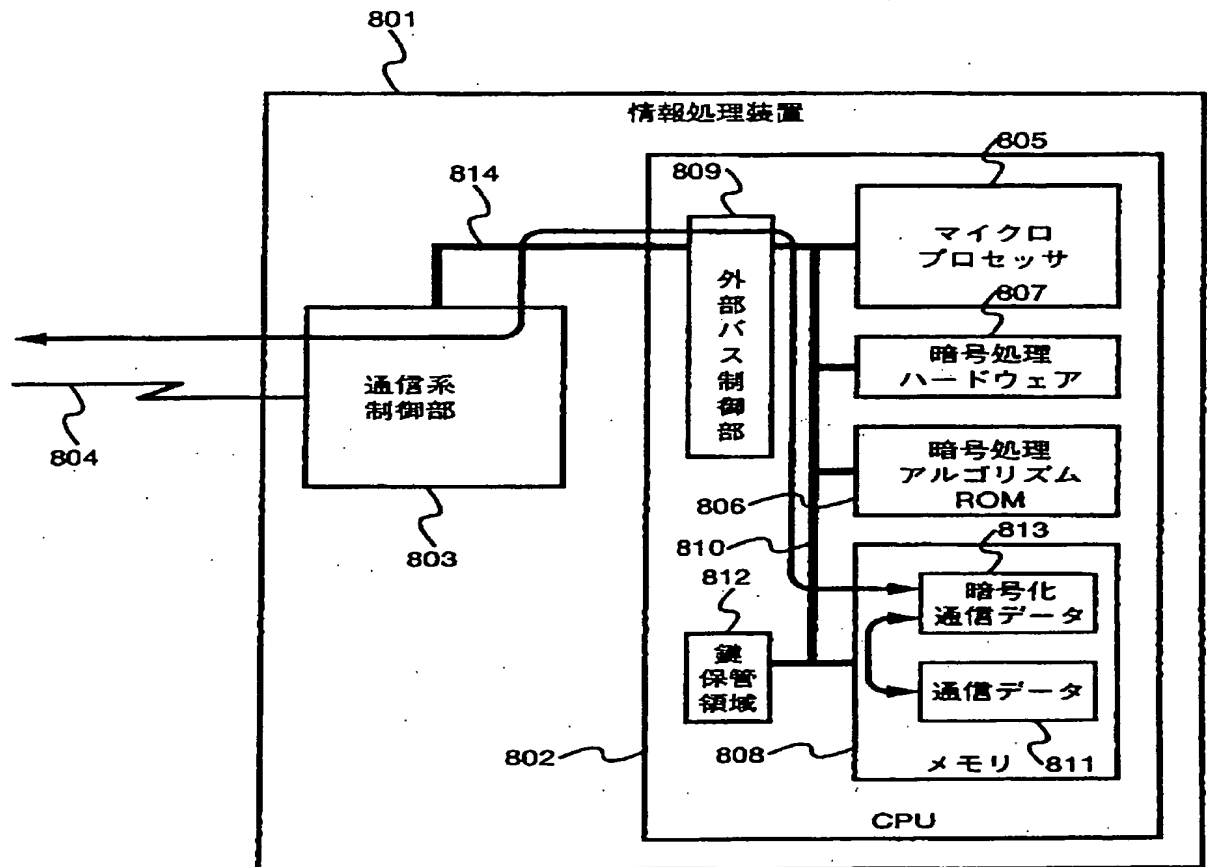
第6図



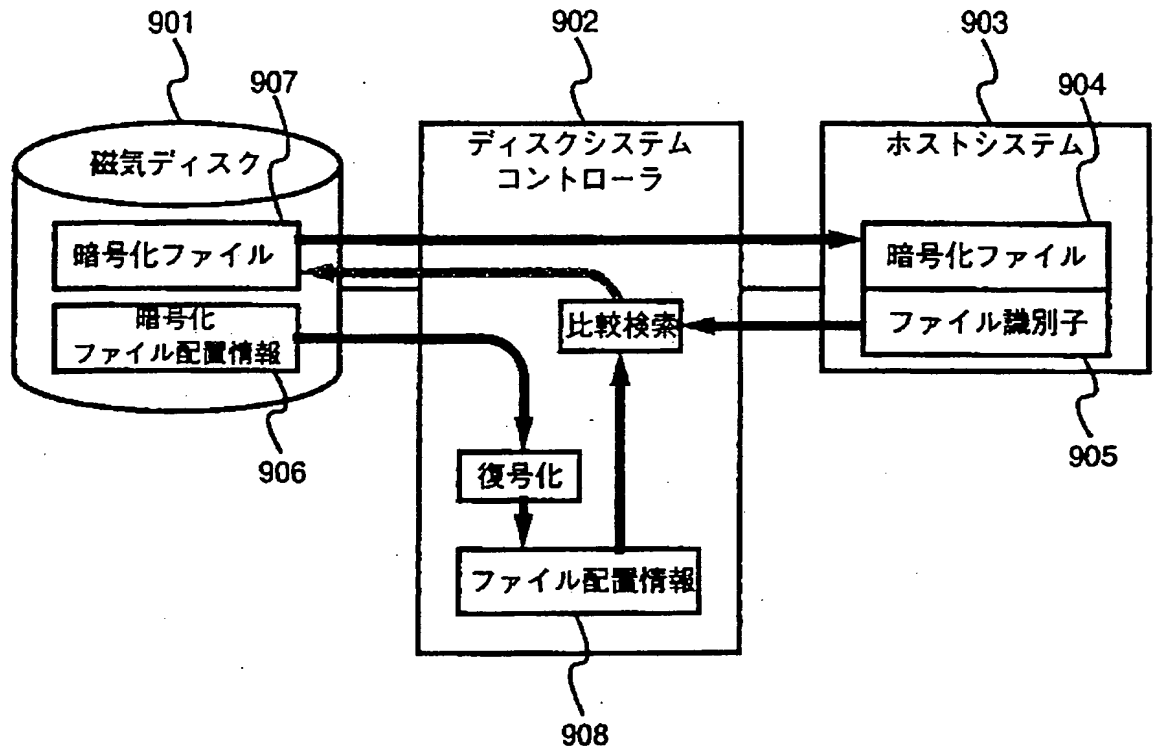
第7図



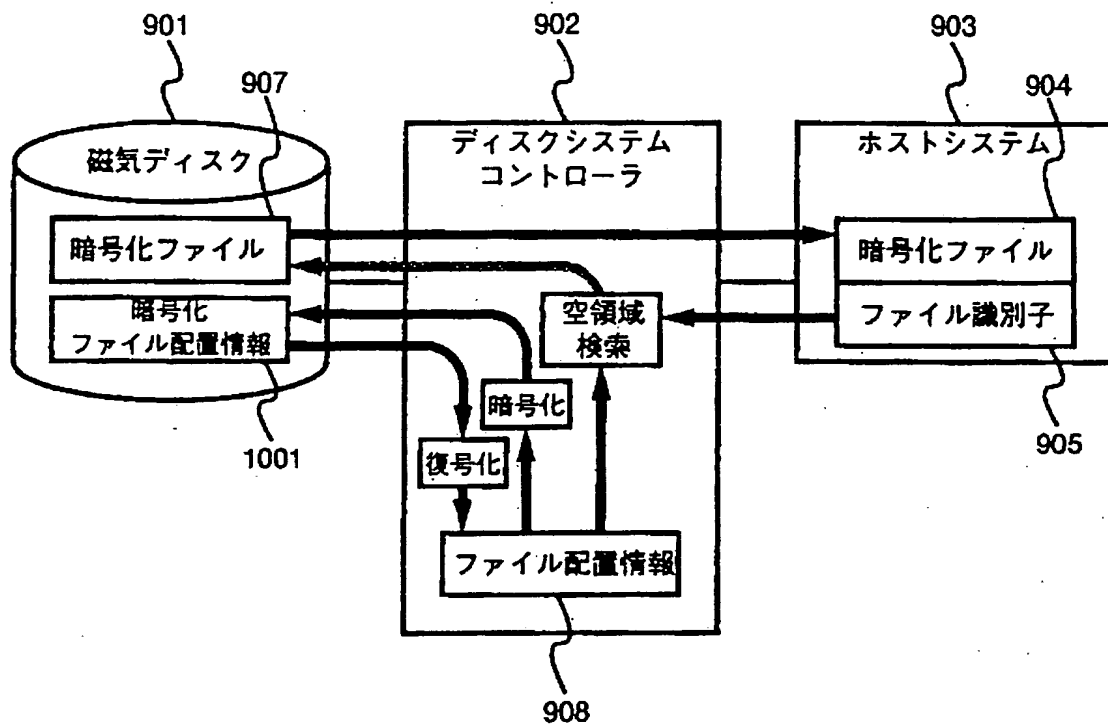
第8図



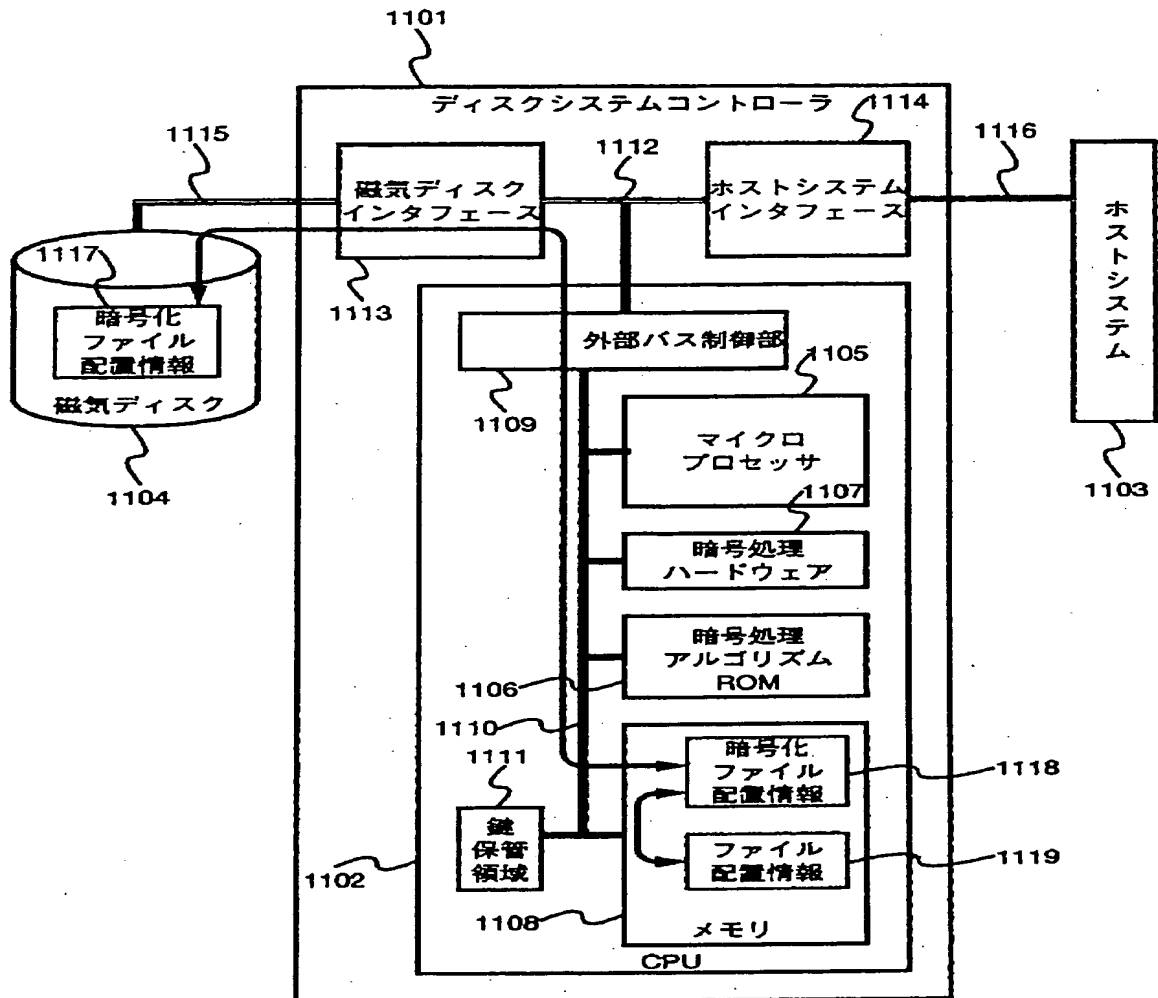
第9図



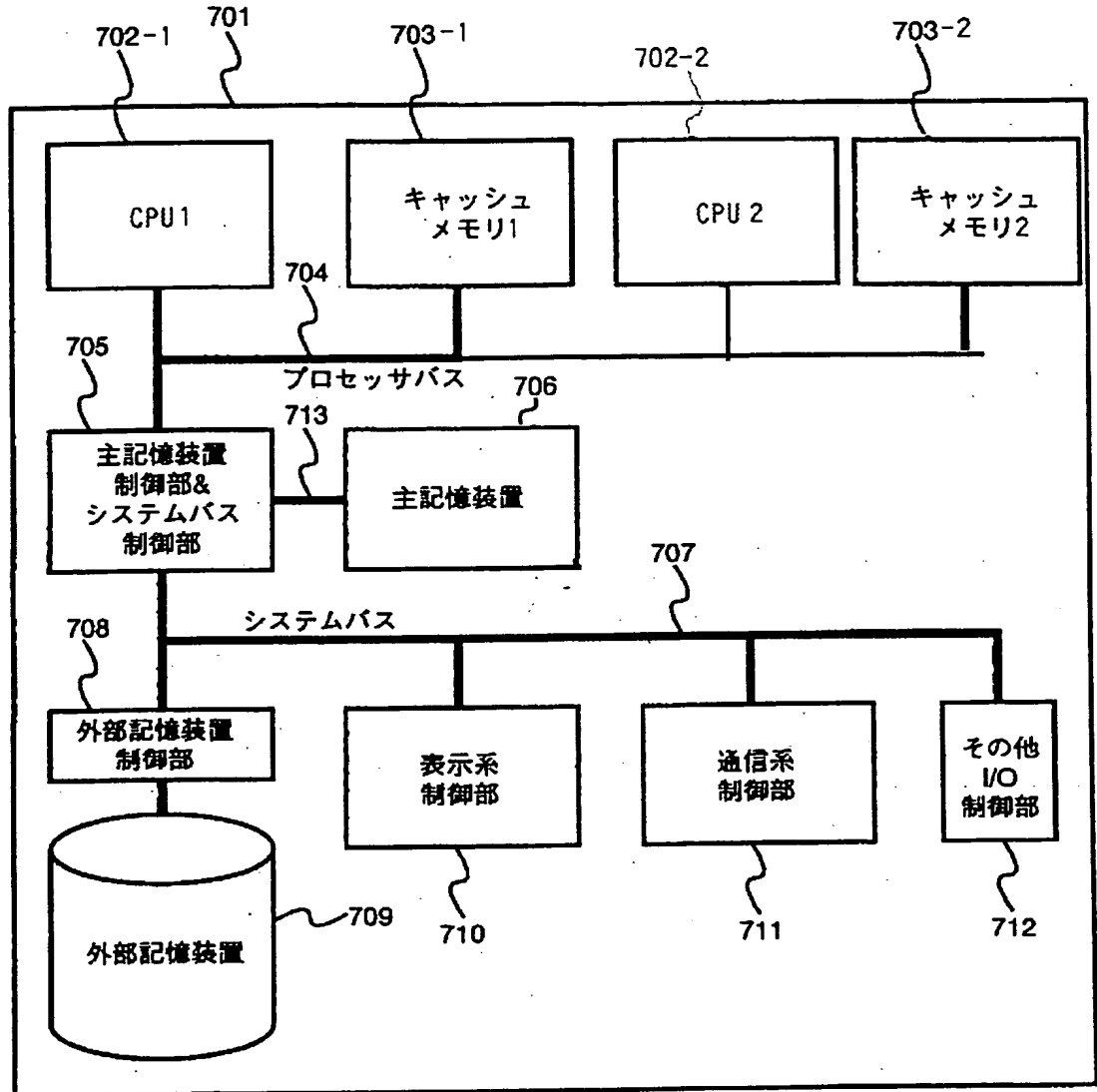
第10図



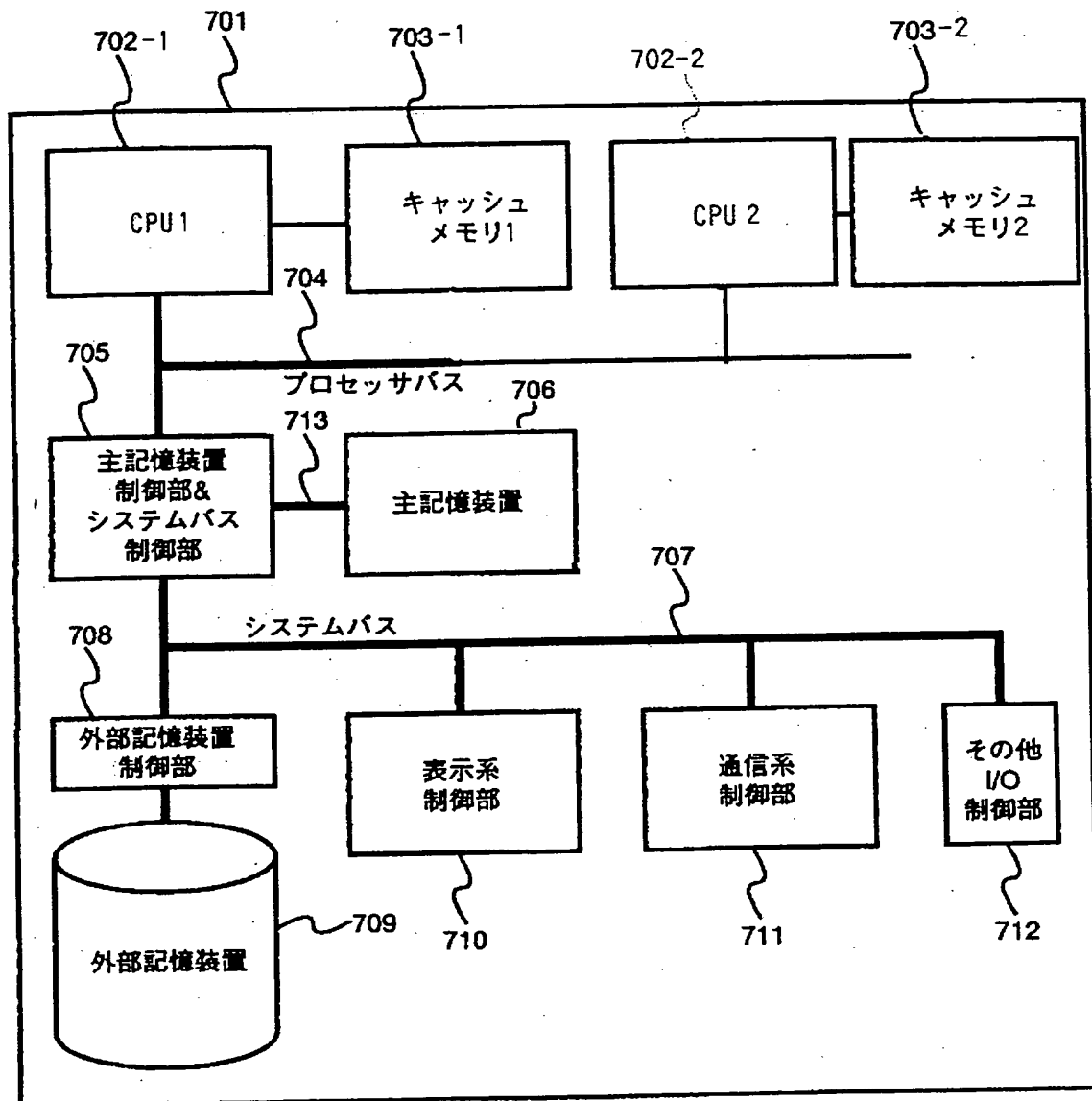
第11図



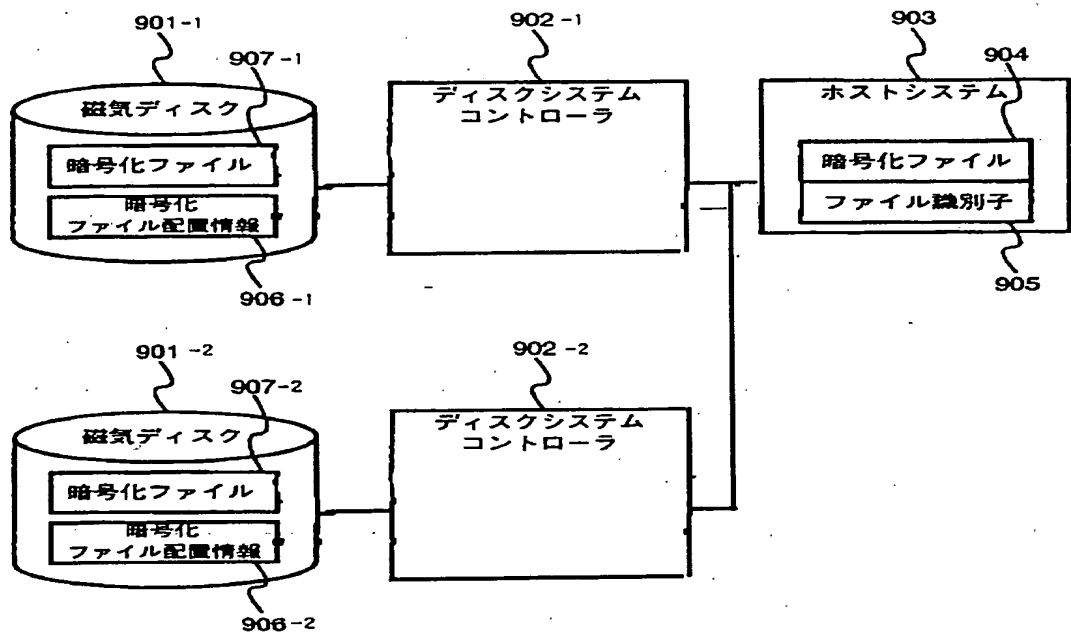
第12図



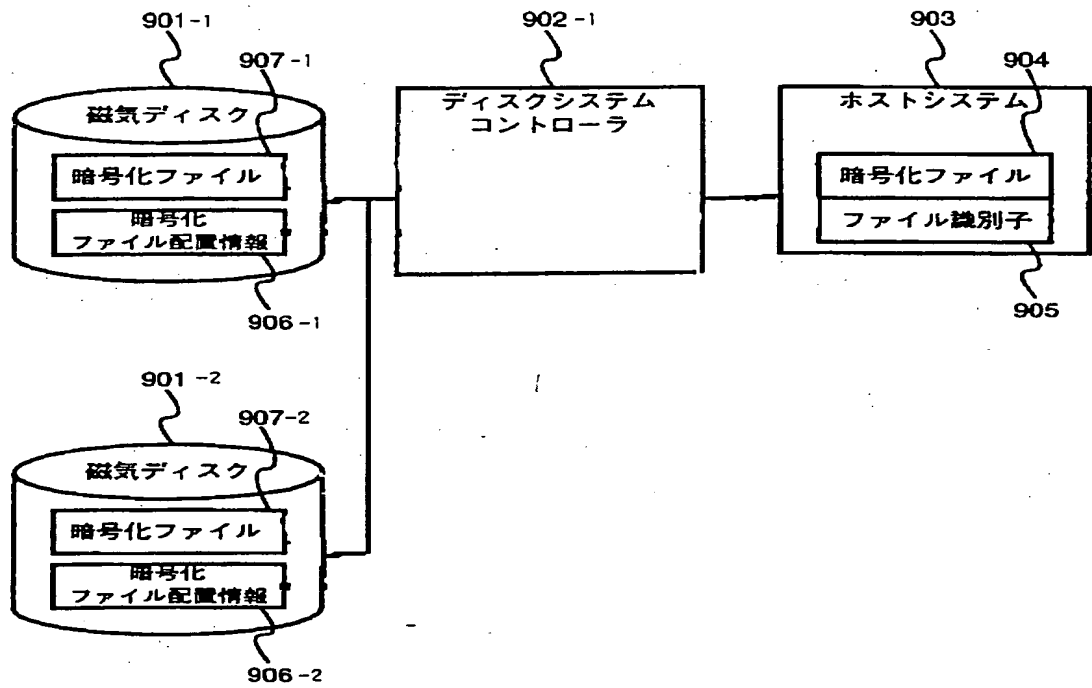
第13図



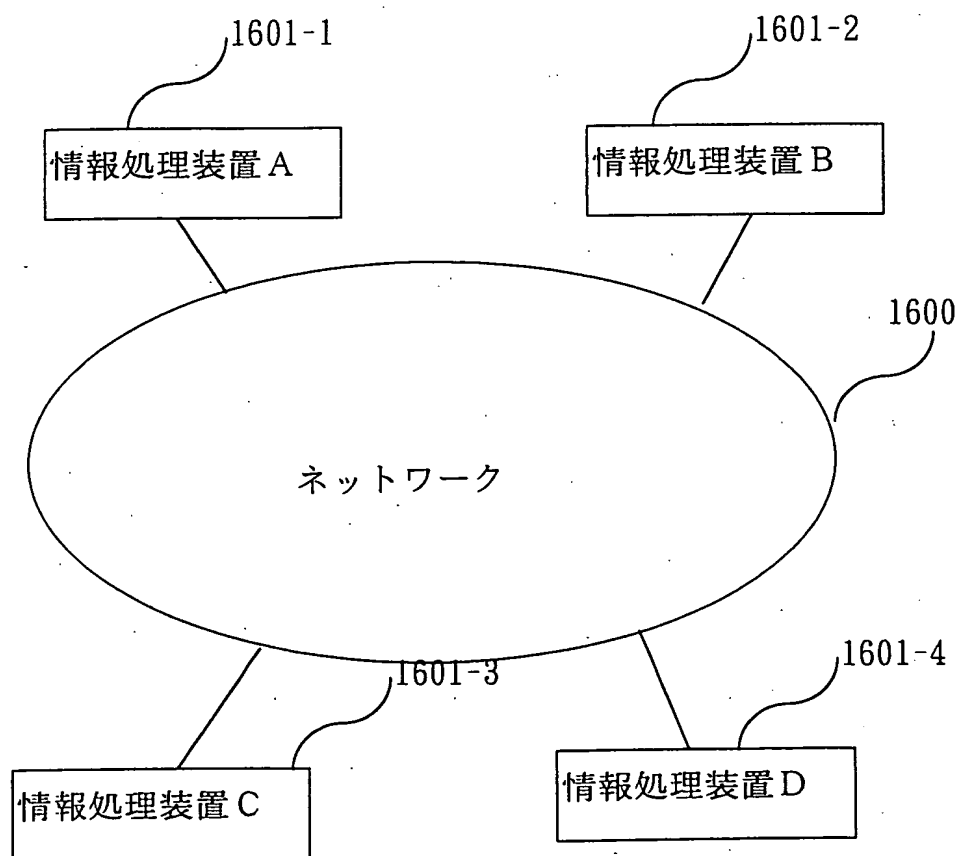
第14図



第15図



第16図



This Page Blank (uspto)